

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号  
特開2000-322280  
(P2000-322280A)

(43)公開日 平成12年11月24日(2000. 11. 24)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テ-マコ-ド*(参考)
G 0 6 F 11/10	3 3 0	G 0 6 F 11/10	3 3 0 Q 5 B 0 0 1
H 0 3 M 13/00		H 0 3 M 13/00	5 J 0 6 5
H 0 4 L 1/00		H 0 4 L 1/00	Z 5 K 0 1 4

審査請求 未請求 請求項の数2 O L (全 4 頁)

(21)出願番号 特願平11-130903

(22)出願日 平成11年5月12日(1999. 5. 12)

(71)出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72)発明者 花木 義孝

大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

(74)代理人 100097445

弁理士 岩橋 文雄 (外2名)

Fターム(参考) 5B001 AA11 AB02 AC01

5J065 AC01 AD11 AF01 AF03 AG01

AH03

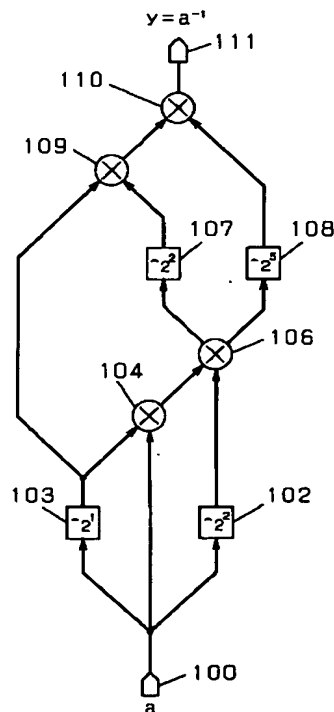
5K014 AA05 BA08 EA01 EA02

(54)【発明の名称】 ガロア体演算方法

(57)【要約】

【課題】 ガロア体の逆元を生成するガロア体演算器を実現するにあたり、高速なパイプライン動作を実現しつつ、回路規模の小さなガロア体演算器を実現することを目的とする。

【解決手段】 図1に示すようなガロア体演算の乗算器によるランダムロジックによって、逆元ROMを用いることなく、ガロア体GF(2<sup>8</sup>)上の逆元を生成する。これにより、ROMを用いることがないので、スループットの高い、高速なガロア体演算をすることができるという効果がある。



## 【特許請求の範囲】

【請求項 1】 第 1 のガロア体の元を 2 乗して第 2 のガロア体の元を生成するステップと、

前記第 1 のガロア体の元を 4 乗して第 3 のガロア体の元を生成するステップと、

前記第 1、第 2 のガロア体の元とをガロア体乗算して第 4 のガロア体の元を生成するステップと、

前記第 3、第 4 のガロア体の元とをガロア体乗算して第 5 のガロア体の元を生成するステップと、

前記第 5 のガロア体の元を 4 乗して第 6 のガロア体の元を生成するステップと、

前記第 5 のガロア体の元を 3 2 乗して第 7 のガロア体の元を生成するステップと、

前記第 2、第 6 のガロア体の元とをガロア体乗算して第 8 のガロア体の元を生成するステップと、

前記第 7、第 8 のガロア体の元とをガロア体乗算して前記第 1 のガロア体の元の逆元を生成するステップとを備えることを特徴とするガロア体演算方法。

【請求項 2】 請求項 1 記載のガロア体演算方法において、

第 10 のガロア体の元を入力し、第 2 のガロア体の元とガロア体乗算を行い、新たな第 2 のガロア体の元を生成するガロア体乗算ステップを更に備えることを特徴とするガロア体演算方法。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】蓄積装置、情報通信などの分野において、誤り訂正符号に関する技術の応用が盛んである。本発明は、誤り訂正符号として有力なリード・ソロモン符号の復号・符号化に必要となる、ガロア体演算方法に関するものである。

## 【0002】

【従来の技術】従来、ガロア体  $GF(2^n)$  上の逆元生成器は、逆元 ROM と呼ばれる ROM を用いて構成されていた。逆元 ROM には、ガロア体上の逆元がデータとして格納されている。

【0003】図 2 に、従来のガロア体上の逆元生成器の構成を示す。図 2 において、100 は入力端子、111 は出力端子、112 は逆元 ROM である。

【0004】図 3 の構成によるガロア体逆元生成器の動作を、以下に説明する。まず、ガロア体演算方法への入力が逆元 ROM 112 に入力され、その逆元が逆元 ROM 112 から出力され、端子 111 から出力される。

【0005】従来の構成では、以上のようにして、ガロア体逆元生成器を得ていた。

【0006】図 4 に、従来のガロア体除算器の構成を示す。図 4 において、100、101 は入力端子、111 は入力端子、112 は端子 101 から入力されたガロア体  $GF(2^8)$  上の逆数を出力する逆元 ROM、114 は端子 110 からの入力と逆元 ROM 112 の出力を

乗ずるガロア体乗算器である。

【0007】図 4 の構成によるガロア体除算器の動作を、以下に説明する。まず、ガロア体演算方法へ除数として与えられた入力  $b$  が逆元 ROM 112 に入力され、その逆元  $b^{-1}$  が逆元 ROM 112 から出力される。ガロア体乗算器 114 では、逆元 ROM から出力された除数の逆元  $b^{-1}$  と端子 100 から入力された被除数  $a$  とを乗ずることによってガロア体除算の結果  $b/a$  が生成され、端子 111 から出力される。

【0008】従来の構成では、以上のようにして、ガロア体除算器を得ていた。

## 【0009】

【発明が解決しようとする課題】以下に、従来のガロア体演算方法の構成における課題について論ずる。従来の構成では、ガロア体上の逆元を生成するため、あるいは、ガロア体上の除算を実行するためには、ガロア体上の逆元を記憶した ROM が必要であった。そのため、ガロア体演算方法にパイプライン構造をもたせて、ROM のアクセス速度以上のスループットを実現するには、複数の ROM をインターリーブさせる必要があり、高速なパイプライン動作を実現しつつ回路規模の小さなガロア体演算方法を得るのが困難である、という課題があった。また、ガロア体の原始多項式に対応した逆元 ROM が必要であるため、複数の原始多項式に対応するためには、原始多項式の数と同数の逆元 ROM が必要となる。そのため、複数の原始多項式に対応しつつ回路規模の小さなガロア体演算方法を得るのが困難である、という課題があった。また、ガロア体上の逆元を記憶するための専用 ROM を実装する必要があるため、ゲートアレイや FPGA などを実装するのが困難である、という課題があった。

【0010】本発明は、上記のような従来の課題を解決するものであり、ガロア体上の逆元の生成、あるいは、ガロア体上の除算をおこなうガロア体演算方法を実現するにあたり、高速なパイプライン動作を実現しつつ回路規模の小さなガロア体演算方法を提供すること、および、複数の原始多項式に対応しつつなお回路規模の小さなガロア体演算方法を提供すること、および、ゲートアレイや FPGA などにも容易に実装可能なガロア体演算方法を提供することを目的とする。

## 【0011】

【課題を解決するための手段】この目的を達成するために、本発明の請求項 1、および請求項 2 記載のガロア体演算方法は、ガロア体  $GF(2^8)$  上の元を入力する端子と、ガロア体 2 乗回路と、ガロア体 4 乗回路と、ガロア体 3 2 乗回路と、4 つのガロア体乗算回路と、出力端子とで構成されることを特徴とする。

【0012】この構成では、回路がランダムロジックで構成されるため、容易にガロア体演算方法にパイプライン構造を持たせることができる。すなわち、スループット

## 3.

トの高いガロア体演算パイプラインを実現可能である。

【0013】また、この構成では、逆元ROMを必要とせず、回路面積の大部分はガロア体乗算器で占められるが、ガロア体乗算器は回路規模をさほど増大させることなく対応する原始多項式の数を増加させ得る。このため、複数の原始多項式に対応しつつ、回路面積の小さなガロア体演算方法を構成することが可能である。

【0014】また、この構成では、逆元ROMを必要とせず、ゲートアレイやFPGAへの実装が容易である。

【0015】

【発明の実施の形態】以下、本発明の実施の形態について、図面を参照しながら説明する。

【0016】（実施の形態1）図1は、本実施の形態1のガロア体演算方法の構成を示すブロック図である。図1のガロア体演算方法は、ガロア体上の逆元を生成する。

【0017】図1において、100はガロア体GF(2<sup>8</sup>)上の元aを入力する端子、102は端子100からの入力aを4乗するガロア体4乗回路、103は端子100からの入力aを2乗するガロア体2乗回路、104は端子100からの入力aとガロア体2乗回路103からの出力(a<sup>2</sup>)を乗ずるガロア体乗算器、106はガロア体4乗回路102からの出力(a<sup>4</sup>)とガロア体乗算器104からの出力(a<sup>3</sup>)を乗ずるガロア体乗算器、107はガロア体乗算器106の出力(a<sup>7</sup>)を4乗するガロア体4乗回路、108はガロア体乗算器106の出力(a<sup>7</sup>)を32乗するガロア体32乗回路、109はガロア体2乗回路103の出力(a<sup>2</sup>)とガロア体4乗回路107の出力(a<sup>28</sup>)を乗ずるガロア体乗算器、110はガロア体32乗回路108の出力(b x a<sup>224</sup>)とガロア体乗算器109の出力(a<sup>30</sup>)を乗ずるガロア体乗算器、111はガロア体乗算器110の出力(a<sup>254</sup>=a<sup>-1</sup>)を出力する端子である。

【0018】以上のように構成された実施の形態1のガロア体演算方法の動作を、以下に説明する。まず、ガロア体GF(2<sup>8</sup>)上の元aが端子100から入力され、ガロア体4乗回路102においてa<sup>4</sup>が生成され、ガロア体2乗回路103においてa<sup>2</sup>が生成され、ガロア体乗算器104においてa<sup>3</sup>が生成され、ガロア体乗算器106においてa<sup>7</sup>が生成され、ガロア体4乗回路107においてa<sup>28</sup>が生成され、ガロア体32乗回路108においてa<sup>224</sup>が生成され、ガロア体乗算器109においてa<sup>30</sup>が生成され、ガロア体乗算器110においてa<sup>254</sup>が生成され、端子111から出力される。これはガロア体演算方法の入力aの逆数a<sup>-1</sup>に等しい。

【0019】以上のようにして、本発明の実施の形態1のガロア体演算方法では、ガロア体GF(2<sup>8</sup>)上の逆数を得る。

## 4.

【0020】ここで、以上の構成において、演算遅延を考慮して、適切な場所にラッチを挿入することにより、パイプライン動作をさせ、スループットを向上させることができる。よって逆元ROMを用いた場合に比べ、スループットは向上するという効果がある。

【0021】（実施の形態2）図2は、本実施の形態2のガロア体演算方法の構成を示すブロック図である。図2のガロア体演算方法は、ガロア体GF(2<sup>8</sup>)上の除算をおこなう。

10 【0022】図2において、100はガロア体GF(2<sup>8</sup>)上の元aを入力する端子、101はガロア体GF(2<sup>8</sup>)上の元bを入力する端子、102は端子100からの入力aを4乗するガロア体4乗回路、103は端子100からの入力aを2乗するガロア体2乗回路、104は端子100からの入力aとガロア体2乗回路103からの出力(a<sup>2</sup>)を乗ずるガロア体乗算器、105は端子101からの入力bとガロア体乗算器103の出力(a<sup>2</sup>)とを乗ずるガロア体乗算器、106はガロア体4乗回路102からの出力(a<sup>4</sup>)とガロア体乗算器104からの出力(a<sup>3</sup>)を乗ずるガロア体乗算器、107はガロア体乗算器106の出力(a<sup>7</sup>)を4乗するガロア体4乗回路、108はガロア体乗算器106の出力(a<sup>7</sup>)を32乗するガロア体32乗回路、109はガロア体2乗回路103の出力(a<sup>2</sup>)とガロア体4乗回路107の出力(a<sup>28</sup>)を乗ずるガロア体乗算器、110はガロア体32乗回路108の出力(b x a<sup>224</sup>)とガロア体乗算器109の出力(b x a<sup>30</sup>)を乗ずるガロア体乗算器、111はガロア体乗算器110の出力(b x a<sup>254</sup>=b/a)を出力する端子である。

20 【0023】以上のように構成された実施の形態1のガロア体演算方法の動作を、以下に説明する。まず、ガロア体GF(2<sup>8</sup>)上の元aが端子100から入力され、ガロア体4乗回路102においてa<sup>4</sup>が生成され、ガロア体2乗回路103においてa<sup>2</sup>が生成され、ガロア体乗算器104においてa<sup>3</sup>が生成され、ガロア体乗算器105においてb x a<sup>2</sup>が生成され、ガロア体乗算器106においてa<sup>7</sup>が生成され、ガロア体4乗回路107においてa<sup>28</sup>が生成され、ガロア体32乗回路108においてa<sup>224</sup>が生成され、ガロア体乗算器109においてb x a<sup>30</sup>が生成され、ガロア体乗算器110においてb x a<sup>254</sup>が生成され、端子111から出力される。これはb/aに等しい。

【0024】以上のようにして、本発明の実施の形態2のガロア体演算方法では、ガロア体GF(2<sup>8</sup>)上の除算をおこなう。

50 【0025】ここで、以上の構成において、演算遅延を考慮して、適切な場所にラッチを挿入することにより、パイプライン動作をさせ、スループットを向上させるこ

とができる。よって逆元ROMを用いた場合に比べ、スループットは向上するという効果がある。

#### 【0026】

【発明の効果】以上のように、本発明によれば、入力する端子と、ガロア体2乗回路と、ガロア体4乗回路と、ガロア体32乗回路と、5つのガロア体乗算回路と、出力端子とを備えることにより、容易にパイプライン化が可能で、回路規模を増大させることなく複数の原始多項式に対応可能で、ゲートアレイやFPGAへの実装も容易なガロア体演算方法を得ることができる。

#### 【図面の簡単な説明】

【図1】本発明の実施の形態1に係るガロア体逆元生成器の構成を示すブロック図

【図2】本発明の実施の形態2に係るガロア体除算器の構成を示すブロック図

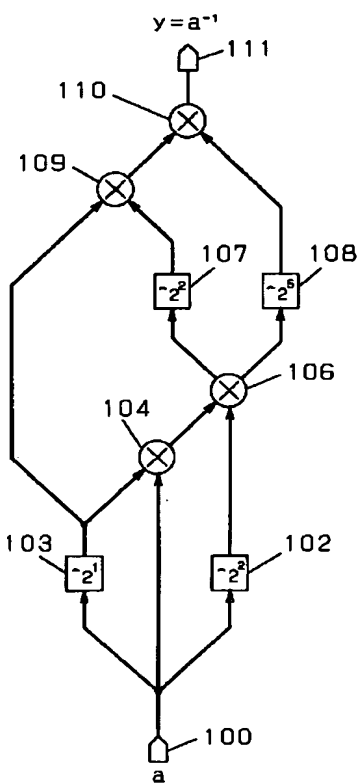
【図3】従来のガロア体逆元生成器の構成を示すブロック図

【図4】従来のガロア体除算器の構成を示すブロック図

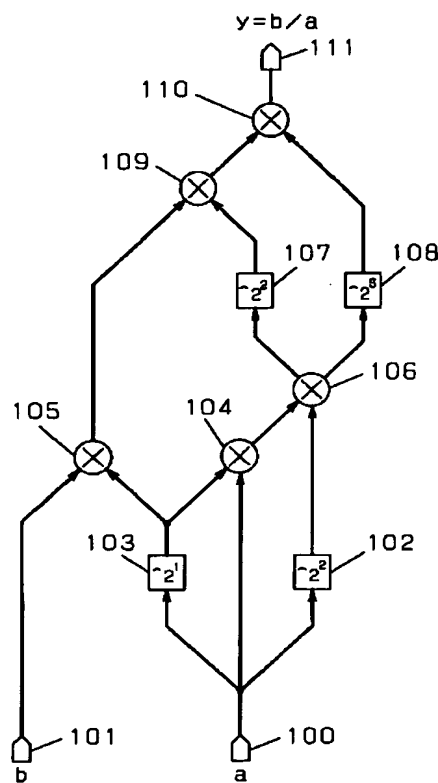
#### 【符号の説明】

- 100～101 入力端子
- 102 ガロア体4乗回路
- 103 ガロア体2乗回路
- 104～106 ガロア体乗算器
- 107 ガロア体4乗回路
- 108 ガロア体32乗回路
- 109～110 ガロア体乗算器
- 111 出力端子
- 112 逆元ROM
- 114 ガロア体乗算器

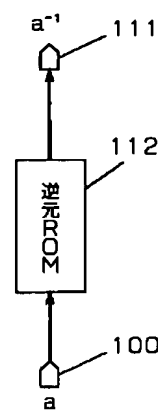
【図1】



【図2】



【図3】



【図4】

